Securing the cloud with homomorphic encryption



Research Directorate staff

he word homomorphic has roots in Greek and loosely translates as "same shape" or "same form." In relation to cryptography, the concept is that operations can be performed on encrypted data without sharing the secret key needed to decrypt the data. Homomorphic encryption has great utility in cloud computing, particularly for those that wish to house encrypted data on cloud providers' servers.

A major hurdle to the adoption of cloud-based services is security. Cloud users, particularly at the enterprise and government level, are concerned with losing control of, or just plain losing, their data once it is placed in the cloud. The abstractness of cloud storage makes it difficult for consumers to feel comfortable that their data is well protected by cloud service providers. Encryption could alleviate this issue. However, if you want to manipulate your encrypted data in the cloud, the secret key to decrypt your data must be shared with the cloud provider. This sort of defeats the idea of a secret key. Sharing this key of course would allow the current cloud provider (or future provider if the service changes hands) access to your data. The answer to this problem could be homomorphic encryption.

For example, a bakery in New York that uses a cloud service provider's infrastructure to host their e-mail wants to search through those e-mails for an order erroneously sent to Hoboken, New Jersey. If the data is plaintext, the subscriber just plugs in a search term (e.g., "cupcakes Hoboken") and views the results. If the data is encrypted, the bakery will need to share the secret key with the cloud provider to access the information stored on the provider's servers to query against the data. Sharing that secret key now potentially gives the provider access to the company's data, and if there is a security breach, it may also give cybercriminals access to the data. Homomorphic encryption would allow the bakery's owners to search the encrypted e-mails for items related to the Hoboken mishap and get results as if

querying against the plaintext data, without sharing the key.

The idea of homomorphic encryption has been around for about 30 years, and thanks to a significant breakthrough in 2009, the end game of a practical fully homomorphic encryption solution is in sight. There are fully homomorphic encryption solutions that exist today, but because of limitations related mainly to the complexity of computations, these solutions are not considered practical for use with today's applications. These limitations are being addressed, and some say a practical solution could be achieved within a decade. If a practical, fully homomorphic solution can be created, it could be the catalyst that breaks down the security barrier to widespread cloud adoption.

Technical overview

Fully versus somewhat homomorphic encryption

There are two types of homomorphic encryption: fully homomorphic encryption (FHE) and somewhat homomorphic encryption (SHE). Each type differs in the number of operations that can be performed on encrypted data. FHE allows for an unlimited, arbitrary number of computations (both addition and multiplication) to be performed on encrypted data. SHE cryptosystems support a limited number of operations (i.e., any amount of addition, but only one multiplication) and are faster and more compact than FHE cryptosystems [1].

Bootstrapping and lattices

One of the hindrances limiting the feasibility of FHE is managing the so called "noise." Noise, in this case, refers to the distortion of ciphertexts (i.e., encoded text) that occurs after each operation (e.g., addition or multiplication) is performed. As more and more additions and multiplications are performed, the noise level becomes too high, and the resulting ciphertexts become indecipherable. Ciphertexts can be refreshed easily by decrypting them, but the idea behind homomorphic encryption is to not share the secret key required to do the decryption.

Craig Gentry used a process called bootstrapping to overcome this noise problem in SHE solutions. Bootstrapping modifies an SHE solution so it can homomorphically run its own decryption procedure by adding an encryption of the secret key to the public key (see figure 1). This is accomplished by using a sparse subset-sum problem (SSSP) or augmenting the public key with a large set of vectors so that a sparse subset of the vectors will add up to be the secret key.

The idea of bootstrapping calls for double encrypting the data and, as processes run, removing a layer of encryption. Gentry's bootstrapping procedure adds another layer of encryption after a few computations using an encrypted key to unlock the inner layer of scrambling. This process "refreshes" the still-encrypted data and could allow for an infinite number of computations, effectively turning an SHE solution into an FHE solution. However, each extra layer of encryption will increase the overall computational effort needed to complete a query [1, 2, 3].

The downside of Gentry's bootstrapping idea is that it requires huge amounts of computational effort. For example, if the process were to be used by Google to search the web homomorphically, the normal computing time would be multiplied



FIGURE 1. Gentry's bootstrapping method modifies an SHE solution so it can homomorphically run its own decryption procedure by adding an encryption of the secret key to the public key.

by about a trillion, according to Gentry. This extra computing time is one of the reasons that a practical FHE solution is not available for implementation today. Although strides are being made every day to overcome the amount of processing overhead needed to use these solutions, the schemes tend to be difficult to understand and even harder to implement. Also, the rate of improvement that is occurring in this field could make it hard for early adopters to keep up with the pace of innovation [2, 4].

Another important aspect of FHE solutions is their basis on ideal lattices. Ideal lattices are special classes of lattices that are particularly useful in cryptography [5, 6]. Lattice-based encryption schemes are the focus of FHE solutions because they have simple decryption algorithms which could lessen the computational overhead associated with bootstrapping SHEs [7]. Lattice-based schemes are also attractive for FHEs because they are based on worst-case hardness—meaning that there is a very small chance of attacks succeeding against lattice-based schemes [6]. In this regard, lattice-based cryptographic schemes are believed to even be secure against attacks using quantum computers [6].

Trends

As cloud services spread globally, the need for an FHE scheme will become more important and may begin to draw interest from entities using or planning to use the cloud (public or private) to store data. A report from the International Data Corporation (IDC) on global public cloud-enabling IT infrastructure forecasts that from 2013 through 2017, the majority of cloud adopters will be located in the US, followed closely by subscribers in Western Europe. The US dominance in this area is attributed to the availability of reasonably priced broadband access and the fact that most first-to-market cloud services were located in the US. However, IDC sees adoption in emerging markets (especially Asia) exhibiting strong growth with a more widespread distribution of adoption across all regions occurring beyond 2014 [8].

Two US government entities, the Defense Advanced Research Projects Agency (DARPA) and

the Intelligence Advanced Research Projects Activity (IARPA), issued Broad Agency Announcements (BAAs) for a solution that could perform computations on encrypted data (i.e., homomorphic encryption). In April 2011, DARPA awarded approximately \$5 million to Galois, Inc. to be the research integrator for the Programming Computation on Encrypted Data (PROCEED) program. This award was part of a five-year effort by DARPA worth a total of \$20 million.

In December 2010, IARPA issued a request for proposals for a program called Security And Privacy Assurance Research (SPAR). The goal of the both programs is to make it feasible to execute programs on encrypted data without having to decrypt the data first. DARPA's stated goal was to reduce the computing time for an FHE solution by a factor of 10 million [9].

Conclusion

A practical FHE solution would see widespread use by cloud service providers, significantly hardening cloud security and making cloud storage a more viable option for consumers. Some have predicted that, thanks to Gentry's revelation and the momentum that it generated in the world of cryptography, an FHE solution may be feasible in another decade [2]. A Chief Technology Officer in the UK noted that, by applying Moore's law, it would take 40 years before a fully homomorphic search would be as efficient as a Google search today [10].

Researchers worldwide are actively engaged in trying to perfect a practical FHE solution. Recent breakthroughs include a homomorphic encryption scheme from Fujitsu using batch encryption vice the bit-level encryption usually seen in FHE solutions [11]. Also, in June 2013, researchers from the Massachusetts Institute of Technology, the University of Toronto, and Microsoft Research created a three-part encryption scheme that uses homomorphic encryption as well as two other cryptographic techniques (i.e., garbled circuits and attribute-based encryption) [12]. Although these solutions are not commercially available (Fujitsu hopes to market its solution by 2015), they will perpetuate the continued efforts to field a fully functioning FHE solution.



References

- [1] Hayes B. "Alice and Bob in cipherspace." *American Scientist*. 2012;100(5). Available at: http://www.americanscientist.org/issues/pub/2012/5/alice-and-bob-in-cipherspace/5.
- [2] Greenberg A. "IBM's blindfolded calculator." *Forbes.* Jul 2009. Available at: http://www.forbes.com/forbes/2009/0713/breakthroughs-privacy-super-secret-encryption.html.
- [3] Gentry C, Halevi S. "Implementing Gentry's fully-homomorphic encryption scheme." *Cryptology ePrint Archive.* 2011. Available at: http://eprint.iacr.org/2010/520.
- [4] Aguilar-Melchor C, Fau S, Fontaine C, Gogniat G, Sirdey R. "Recent advances in homomorphic encryption." *IEEE Signal Processing Magazine*. 2013. doi: 10.1109/MSP.2012.2230219.
- [5] "Ideal lattice cryptography." *Wikipedia* [last modified 2013 Jan 10]. Available at: http://en.wikipedia.org/wiki/Ideal_lattice_cryptography.
- [6] "Lattice-based cryptography." *Wikipedia* [last modified 2013 Jan 16]. Available at: http://en.wikipedia.org/wiki/Lattice-based_cryptography.
- [7] Gentry C. "A fully homomorphic encryption scheme" [dissertation]. Stanford University; 2009. Available at: http://crypto.stanford.edu/craig/craig-thesis.pdf.

- [8] Turner MJ, Villars RL, Scaramella J, Mehra R, DuBois L, Iacono D, Gillen A, Chen G, Grady J, Grieser T, Eastwood M. "Worldwide public cloud enabling IT infrastructure 2013–2017 forecast." International Data Corporation. 2013. Doc # 240635.
- [9] Greenberg A. "DARPA will spend \$20 million to search for crypto's holy grail." *Forbes*. Apr 2011. Available at: http://www.forbes.com/sites/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/.
- [10] Schneier B. "Homomorphic encryption breakthrough." *Schneier on Security* [blog]. Jul 2009. Available at: https://www.schneier.com/blog/archives/2009/07/homomorphic_enc.html.
- [11] Fujitsu Laboratories Ltd. "Fujitsu develops world's first homomorphic encryption technology that enables statistical calculations and biometric authentication" [press release]. Aug 2013. Available at: http://www.fujitsu.com/global/news/pr/archives/month/2013/20130828-01.html.
- [12] Hardesty L. "Securing the cloud." *MIT news.* Jun 2013. Available at: http://web.mit.edu/newsoffice/2013/algorithm-solves-homomorphic-encryption-problem-0610.html .

The Next Wave is published to disseminate technical advancements and research activities in telecommunications and information technologies. Mentions of company names or commercial products do not imply endorsement by the US Government.

This publication is available online at http://www.nsa.gov/research/tnw/index.shtml. For more information, please contact us at TNW@tycho.ncsc.mil.





